# A Secret Enriched Visual Cryptography

Feng Liu, Weiqi Yan, Peng Li and Chuankun Wu

February 4, 2021

# Content

- Background
- Preliminaries
- Our work

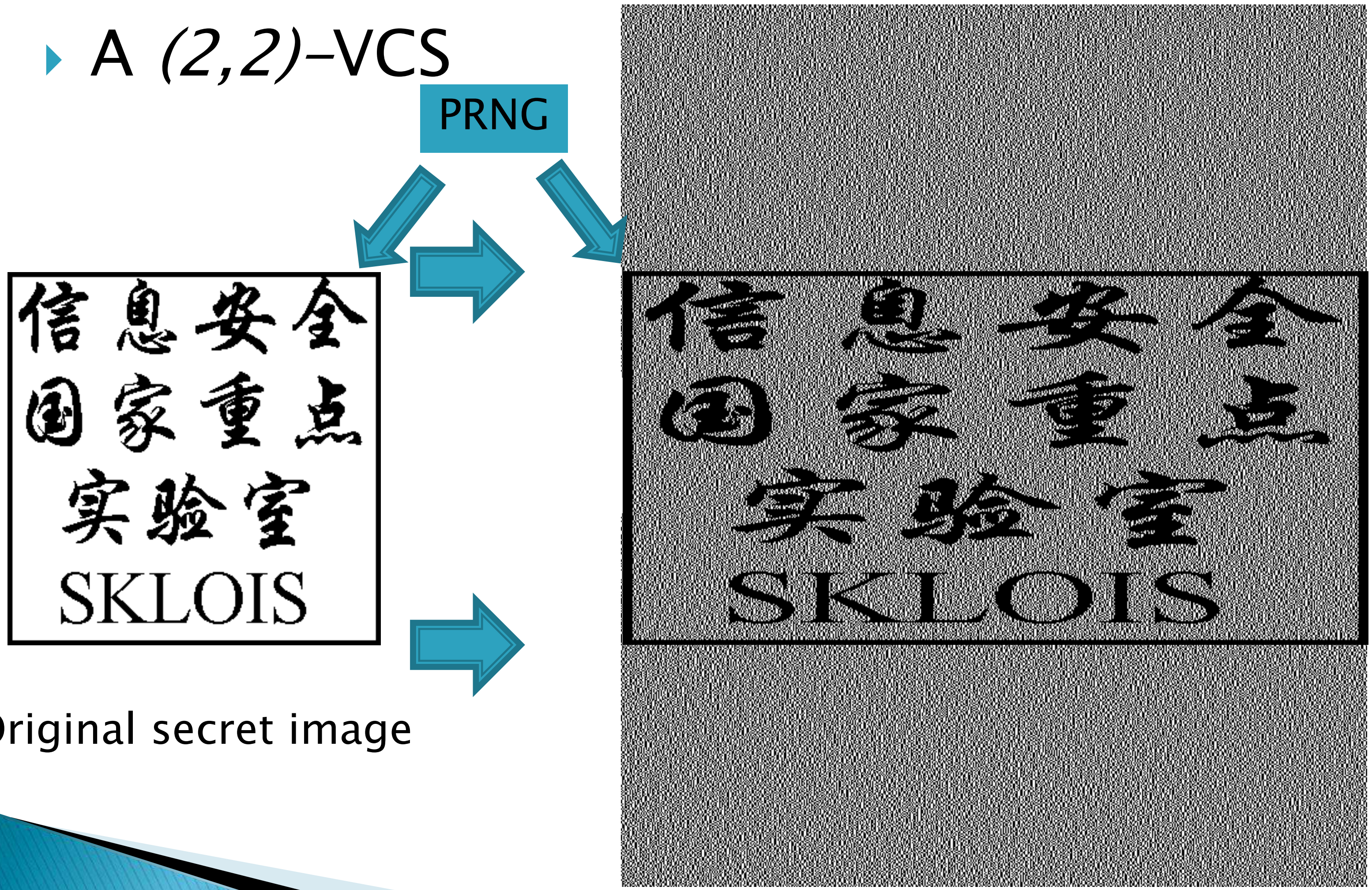
# Background

- Visual Cryptography (VC) has the advantage of "stacking to see", but suffers from large pixel expansion and low information rate.
- Aim of this work: How to let the VC scheme carry more secrets?
- Our approach: Embed the output of a private-key system into the input random numbers of VC.

- Background
- Preliminaries
- Our work

# Overall view of a (2,2)-VCS

- A *(2,2)*-VCS




Original secret image

Share *1*

Share *2*

# Formal Def. of (k, n)- VCS

- Definition 1. Let k, n, m, l and h be non-negative integers satisfying $2 \leq k \leq n$ and $0 \leq l < h \leq m$. The two sets of $n * m$ Boolean matrices $(C_0, C_1)$ constitute a (k, n)-VCS if the following properties are satisfied:
- 1. (Contrast) For any $s \in C_0$, the OR of any k out of the n rows of s, is a vector v that, satisfies $w(v) \leq l$.
- 2. (Contrast) For any $s \in C_1$, the OR of any k out of the n rows of s, is a vector v that, satisfies $w(v) \geq h$.
- 3. (Security) For any $i_1 < i_2 < \ldots < i_t$ in $\{1, 2, \ldots, n\}$ with $t < k$, the two collections of $t * m$ matrices $F_0$ and $F_1$ obtained by restricting each $n * m$ matrix in $C_0$ and $C_1$ to rows $i_1, i_2, \ldots, i_t$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

# Shamir's (t, n)-PSSS

- $f(x) = (a_0 + a_1x + ...+ a_{t-1}x^{t-1}) \bmod p$, where

$a_0$ is the secret from GF(p) and $a_{1,...}$ ,$a_{t-1}$ are randomly drawn element from GF(p).

- Encoding: The n shares can be calculated by f(1) , f(2) , ..., f(n) .

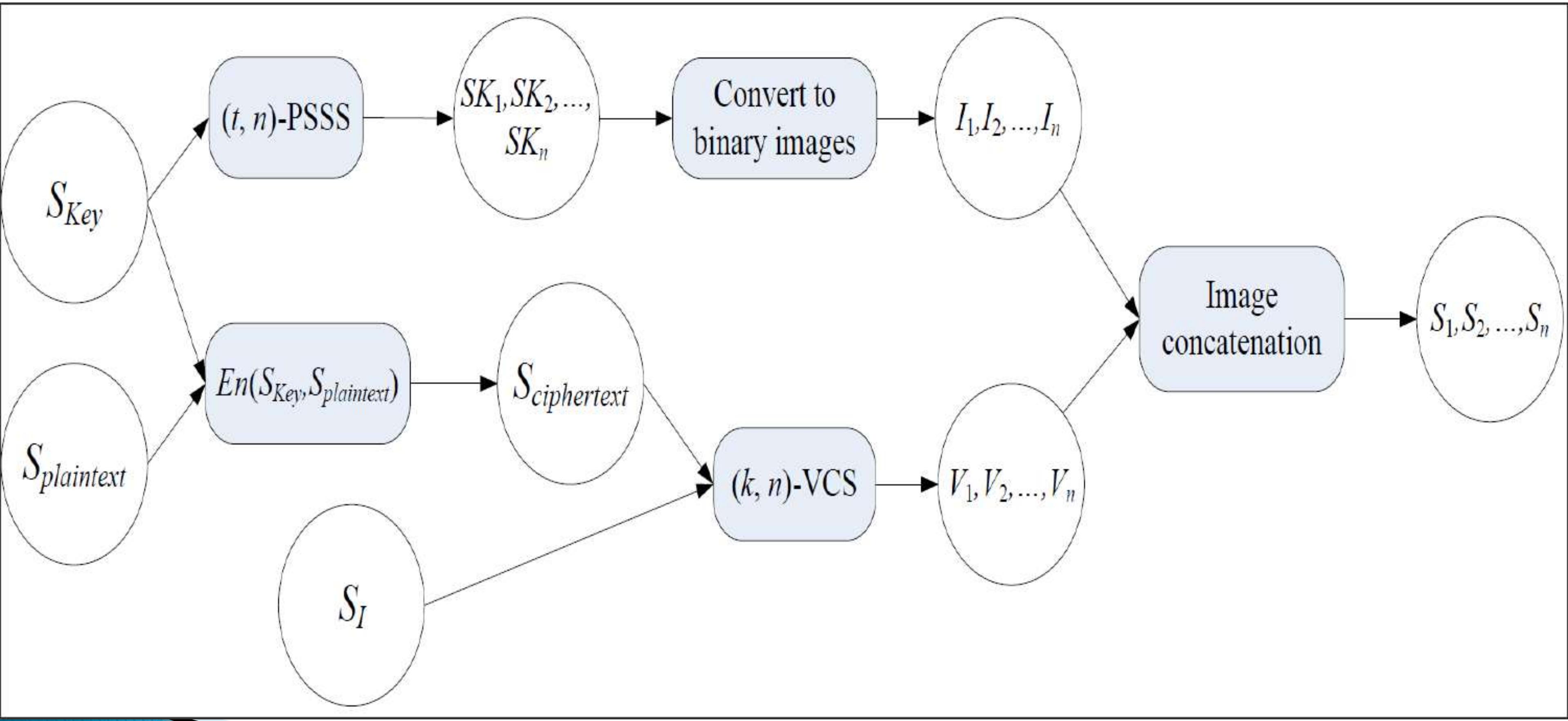
- Decoding: f(x) can be reconstructed from any t of n shares, and hence the secret f(0) can be computed.

- Background
- Preliminaries
- Our work

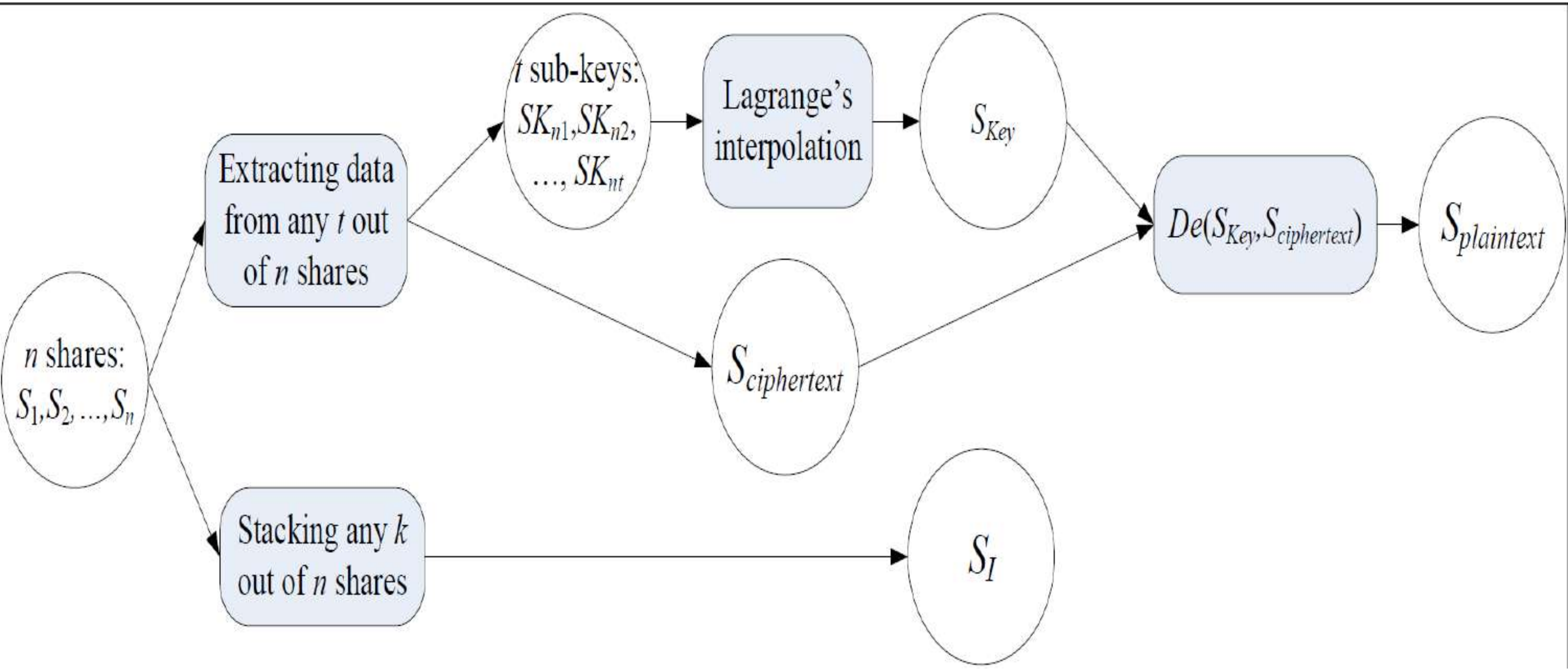
# What is a (k, t, n)–ESSVCS ?

- k: the VCS threshold
- t: the covert data threshold
- n: the number of participants
- $(C_0, C_1)$ require that any t rows can uniquely determine a share matrix
- Generally, it is required that $t \geq k$

# Encoding of ESSVCS



# Decoding of ESSVCS



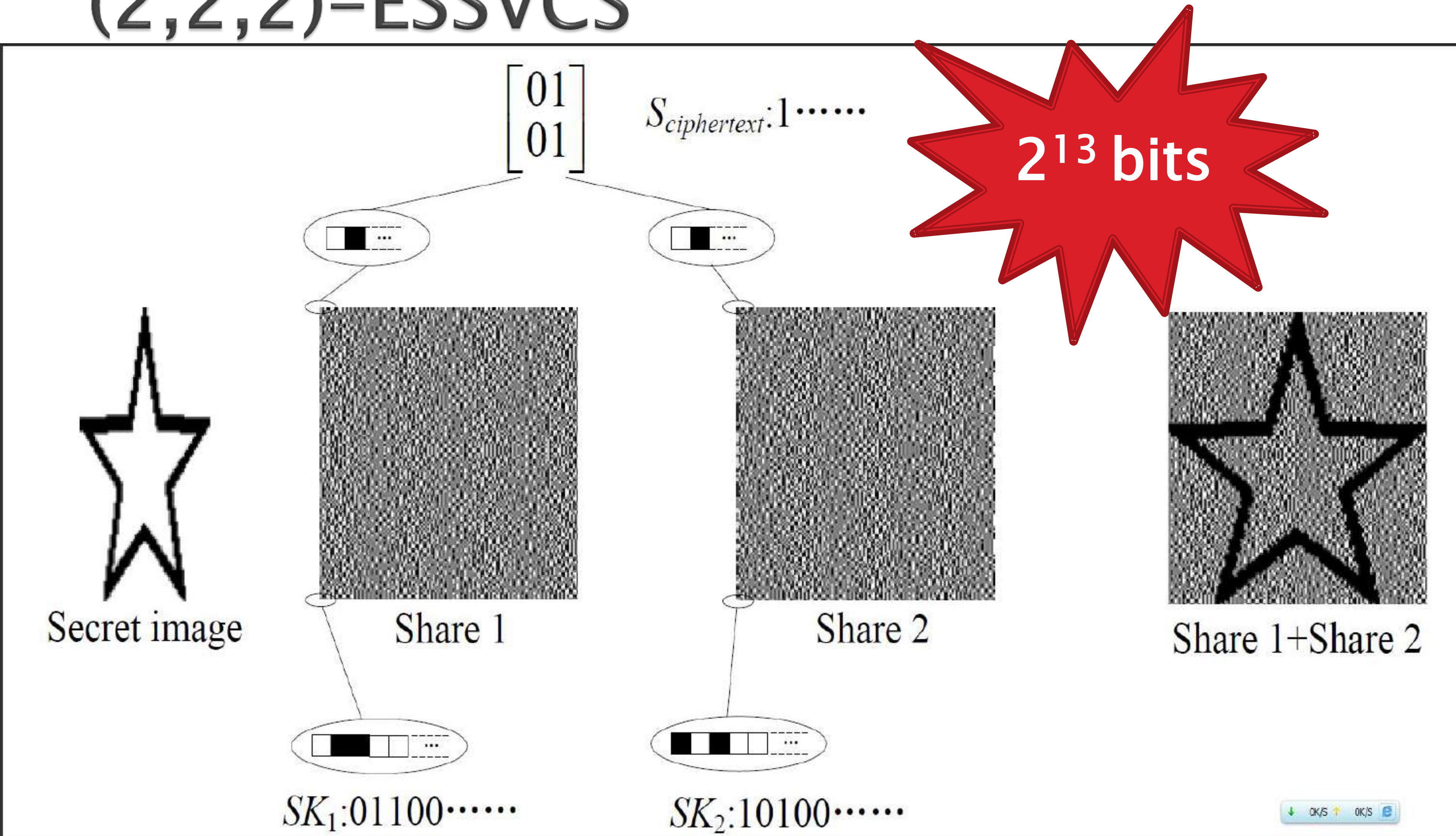
# A (2,2,2)-ESSVCS

- The sets of share matrices of a (2, 2, 2)-ESSVCS are as follows:

$$C_0 = \left\{ \begin{bmatrix} 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \end{bmatrix} \right\} \text{ and } C_1 = \left\{ \begin{bmatrix} 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \end{bmatrix} \right\}$$

- The principle of choosing a share matrix is that: if the random input is 0, we choose the 1st share matrix in $C_0$ or $C_1$; if the random input is 1, we choose the 2nd share matrix.
- From another hand, we also can get to know the random input: if the first share matrix is chosen then the random input is 0, and if the second share matrix is chosen then the random input is 1

# The procedure of the above (2,2,2)-ESSVCS



# Bandwidth of the ESSVCS

- Bandwidth of the ESSVCS is defined by the maximum amount of covert data it carries.
- Theoretically, the amount of covert data carried by a pixel i is $\log_2|C_i|$
- Denote columns in the basis matrix $M_i$ as $c_1,\ldots,c_e$ and multiplicities of these columns as $a_1,\ldots, a_e$. The number of share matrices in $C_i$ is:

$$|C_i| = \frac{(\sum_{i=1}^{e} a_i)!}{\prod_{i=1}^{e} a_i!}$$

- Considering the canonical basis matrices of threshold scheme constructed by Droste, we have the following table:

# Bandwidth of a white pixel

| $k \backslash n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3 | | $4!$ | $\frac{6!}{2!}$ | $\frac{8!}{3!}$ | $\frac{10!}{4!}$ | $\frac{12!}{5!}$ | $\frac{14!}{6!}$ | $\frac{16!}{7!}$ | $\frac{18!}{8!}$ |
| 4 | | | $8!$ | $\frac{15!}{3!2!}$ | $\frac{24!}{6!3!}$ | $\frac{35!}{10!4!}$ | $\frac{48!}{15!5!}$ | $\frac{63!}{21!6!}$ | $\frac{80!}{28!7!}$ |
| 5 | | | | $16!$ | $\frac{30!}{3!(2!)^6}$ | $\frac{48!}{6!(3!)^7}$ | $\frac{70!}{10!(4!)^8}$ | $\frac{96!}{15!(5!)^9}$ | $\frac{126!}{21!(6!)^{10}}$ |
| 6 | | | | | $32!$ | $\frac{70!}{4!(2!)^{21}3!}$ | $\frac{128!}{10!(3!)^{28}6!}$ | $\frac{210!}{20!(4!)^{36}10!}$ | $\frac{320!}{35!(5!)^{45}15!}$ |
| 7 | | | | | | $64!$ | $\frac{140!}{4!(2!)^{28}(3!)^8}$ | $\frac{256!}{10!(3!)^{36}(6!)^9}$ | $\frac{420!}{20!(4!)^{45}(10!)^{10}}$ |
| 8 | | | | | | | $128!$ | $\frac{315!}{5!(3!)^{36}(2!)^{36}4!}$ | $\frac{640!}{15!(6!)^{45}(3!)^{45}10!}$ |
| 9 | | | | | | | | $256!$ | $\frac{630!}{5!(3!)^{45}(2!)^{120}(4!)^{10}}$ |
| 10 | | | | | | | | | $512!$ |

Table 1: The number of share matrices in $C_0$

# Bandwidth of a black pixel

| $k \backslash n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | $2!$ | $3!$ | $4!$ | $5!$ | $6!$ | $7!$ | $8!$ | $9!$ | $10!$ |
| 3 | | $4!$ | $\frac{6!}{2!}$ | $\frac{8!}{3!}$ | $\frac{10!}{4!}$ | $\frac{12!}{5!}$ | $\frac{14!}{6!}$ | $\frac{16!}{7!}$ | $\frac{18!}{8!}$ |
| 4 | | | $8!$ | $\frac{15!}{(2!)^5}$ | $\frac{24!}{(3!)^6}$ | $\frac{35!}{(4!)^7}$ | $\frac{48!}{(5!)^8}$ | $\frac{63!}{(6!)^9}$ | $\frac{80!}{(7!)^{10}}$ |
| 5 | | | | $16!$ | $\frac{30!}{3!(2!)^6}$ | $\frac{48!}{6!(3!)^7}$ | $\frac{70!}{10!(4!)^8}$ | $\frac{96!}{15!(5!)^9}$ | $\frac{126!}{21!(6!)^{10}}$ |
| 6 | | | | | $32!$ | $\frac{70!}{(3!)^7(2!)^7}$ | $\frac{128!}{(6!)^8(3!)^8}$ | $\frac{210!}{(10!)^9(4!)^9}$ | $\frac{320!}{(15!)^{10}(5!)^{10}}$ |
| 7 | | | | | | $64!$ | $\frac{140!}{4!(2!)^{28}(3!)^8}$ | $\frac{256!}{10!(3!)^{36}(6!)^9}$ | $\frac{420!}{20!(4!)^{45}(10!)^{10}}$ |
| 8 | | | | | | | $128!$ | $\frac{315!}{(4!)^9(2!)^{84}(3!)^9}$ | $\frac{640!}{(10!)^{10}(3!)^{120}(6!)^{10}}$ |
| 9 | | | | | | | | $256!$ | $\frac{630!}{5!(3!)^{45}(2!)^{120}(4!)^{10}}$ |
| 10 | | | | | | | | | $512!$ |

Table 2: The number of share matrices in $C_1$

# Bandwidth of the ESSVCS

- Theorem 4. For a secret image $S_I$ which consists of $n_w$ white pixels and $n_b$ black pixels, the bandwidth W of the ESSVCS is $W = \lfloor n_w \log_2 |C_0| + n_b \log_2 |C_1| \rfloor$, and it is achieved when using the $q_a$–pixel encryption model where $q_a = n_w + n_b$.

# Comparison of ESSVCS and TiOISSS

| $k \backslash n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3 | | $\frac{4!}{2!2!}$ | $\frac{6!}{3!3!}$ | $\frac{8!}{4!4!}$ | $\frac{10!}{5!5!}$ | $\frac{12!}{6!6!}$ | $\frac{14!}{7!7!}$ | $\frac{16!}{8!8!}$ | $\frac{18!}{9!9!}$ |
| 4 | | | $\frac{8!}{4!4!}$ | $\frac{15!}{9!6!}$ | $\frac{24!}{16!8!}$ | $\frac{35!}{25!10!}$ | $\frac{48!}{36!12!}$ | $\frac{63!}{49!14!}$ | $\frac{80!}{64!16!}$ |
| 5 | | | | $\frac{16!}{8!8!}$ | $\frac{30!}{15!15!}$ | $\frac{48!}{24!24!}$ | $\frac{70!}{35!35!}$ | $\frac{96!}{48!48!}$ | $\frac{126!}{63!63!}$ |
| 6 | | | | | $\frac{32!}{16!16!}$ | $\frac{70!}{40!30!}$ | $\frac{128!}{80!48!}$ | $\frac{210!}{140!70!}$ | $\frac{320!}{224!96!}$ |
| 7 | | | | | | $\frac{64!}{32!32!}$ | $\frac{140!}{70!70!}$ | $\frac{256!}{128!128!}$ | $\frac{420!}{210!210!}$ |
| 8 | | | | | | | $\frac{128!}{64!64!}$ | $\frac{315!}{175!140!}$ | $\frac{640!}{384!256!}$ |
| 9 | | | | | | | | $\frac{256!}{128!128!}$ | $\frac{630!}{315!315!}$ |
| 10 | | | | | | | | | $\frac{512!}{256!256!}$ |

Table 3: The number of share matrices with different types in Lin et al.'s TiOISSS

*Thank you for your attention*

Any questions?